AF
JFW

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	26

Application Number	10/040,573
Filing Date	11-02-2001
First Named Inventor	FENTON
Art Unit	2134
Examiner Name	POLTORAK
Attorney Docket Number	103036.00014

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☑ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

APPEAL BRIEF (24pp)
Extension Petition (1p)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	JACKSON WALKER L.L.P.		
Signature	/Joseph P Lally/		
Printed name	JOSEPH P LALLY		
Date	MAY 29, 2007	Reg. No.	38,947

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	/Joseph P Lally/		
Typed or printed name	JOSEPH P LALLY	Date	MAY 29, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Fenton *et al.*
Serial No.:	10 #040573
Date Filed:	November 2, 2001
Confirmation No.:	2730
Group Art Unit:	2134
Examiner:	Poltorak, Peter
Title:	***Method and System for Secure Communication***

MAIL STOP – APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Further to a Notice of Appeal and a Pre Appeal Brief Request for Review submitted on February 28, 2007, and a Notice of Panel Decision from Pre-Appeal Brief Review mailed March 28, 2007, Appellant hereby submits this appeal brief according to § 41.37.

A petition extending the period for submission is submitted herewith.

I. REAL PARTY IN INTEREST

The real party in interest is:

Sterling Commerce, Inc.
4600 Lakehurst Court
Dublin, Ohio 43017

by virtue of an assignment as duly recorded on November 2, 2001, at Reel 012469 and Frame 0511 in the Assignment Branch of the U.S. Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision regarding this appeal.

III. STATUS OF CLAIMS

Status	Claims
Rejected:	1-5, 8-10, 14, 21-29, 33-39, 41-43, and 47-55
Canceled:	6-7, 11-13, 15-20, 30-32, 40, and 44-46
Withdrawn:	56-73

The claims being appealed are: 1-5, 8-10, 14, 21-29, 33-39, 41-43, and 47-55.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In the summary below, paragraph references refer to paragraph numbers as shown in the published application, U.S. Patent Application No. 20030088789 A1. Reference numerals from the drawings are indicated by a "#" symbol and, in some instances, an identification of the specific drawing figure. The reference (#X) refers to the unnumbered second proxy shown in FIG. 1 as the VPP connected via dashed line #44 to PSM #43.

Claim 1 recites a method for secure communication including generating, see, e.g., [0037] a plurality of virtual private proxies (VPPs) (FIG. 1 #35) based on an agreement (FIG. 1 #24) between a first entity (FIG. 1 #11) and a second entity (FIG. 1 #12) and associating, see, e.g., [0037] a first VPP (#35) with the first entity (#11) and a second VPP (#X) with the second entity #12. The method also includes monitoring, see, e.g., [0038] data at the first VPP (#35) associated with the first entity (#11) and determining, see, e.g., [0038] whether the data violates the agreement #24. When the monitored data violates the agreement, the method disallows, see, e.g., [0038] communication of the data from the first VPP (#35) to the second VPP (#X).

Claim 14 recites a system (FIG. 1 #10), (FIG. 2 #10) for secure communication including logic, see, e.g., [0023], [0024] stored on a medium and configured to generate, see, e.g., [0037] a plurality of virtual private proxies (VPPs) (#35) based on an agreement (#24) between a first entity (#11) and a second entity (#12) and associate, see, e.g., [0037] a first VPP (#35) with the first entity (#11) and a second VPP (#X) with the second entity (#12). The logic is further configured to monitor, see, e.g., [0038] data at the first VPP (#35) associated with the first entity (#11) and determine, see, e.g., [0038] whether the data violates the agreement (#24). The system (#10) disallows, see, e.g., [0038] communication of the data from the first VPP (#35) to the second VPP (#X) when the data violates the agreement.

Claim 26 recites a method for secure communication including generating, see, e.g., [0037] a first virtual private proxy (VPP) (#35) associated with a first entity (#11) and generating, see, e.g., [0037] a second VPP (#X) associated with a second entity (#12). The

method monitors, see, e.g., [0038] communications between the first VPP (#35) and the second VPP (#X) based on an agreement (#24) for electronic data exchange between, see, e.g., [0015] the first and second entities. The method responds to violations of the agreement based on the agreement., see, e.g., [0069]

Claim 41 recites a system for secure communication including logic, see, e.g., [0023], [0024] stored on storage and configured to generate, see, e.g., [0037] a first virtual private proxy (VPP) (#35) associated with a first entity (#11), generate a second VPP (#X) associated with a second entity (#12), and monitor, see, e.g., [0020] communications between the first VPP (#35) and the second VPP (#X) based on an agreement (#24) for electronic data exchange, see, e.g., [0015] between the first and second entities. The system responds to violations of the agreement based on the agreement., see, e.g., [0069]

Claim 55 recites a method for secure communication comprising generating, see, e.g., [0037] a plurality of virtual private proxies (VPPs) (#35) based on an agreement, see, e.g., [0024] between a first entity (#11) and a second entity #12. The agreement (#24) includes, see, e.g., [0042] a document exchange protocol indication (FIG. 3 #58) and a process specification document indication (FIG. 3 #60). The method includes associating, see, e.g., [0037] a first VPP (#35) with the first entity (#11) and a second VPP (#X) with the second entity #12, where the first VPP (#35) includes a logical representation of a logical access point between the first entity (#11) and a secure switch (#14), see, e.g., [0027]. The method monitors, see, e.g., [0020] data at the first VPP (#35) associated with the first entity (#11) and examines, see, e.g., [0020] the data with respect to the agreement (#24) at the first VPP (#35). The method determines, see, e.g., [0038] whether the data is allowed by the agreement (#24), indicates a violation when the data does not conform to the agreement (#24), and disallows communication of the data from the first VPP (#35) to the second VPP (#X) when the data violates the agreement., see, e.g., [0020]

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 1-4, 14, 24-26, 28-29, 37, 41, 43, and 52-54 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent No. 6,148,290 issued to Dan *et al.* ("Dan") in view of U.S. Patent No. 6,684,329 issued to Epsteine *et al.* ("Epsteine").

Whether Claims 8-10, 21-23, 27, 33-36, 42, and 55 are unpatentable over Dan in view of Epsteine, and further in view of U.S. Patent Publication 2002 #0178103 ("Dan '103").

VII. ARGUMENT

The Section 103(a) rejection of Claims 1-4, 14, 24-26, 28-29, 37, 41, 43, and 52-54 as unpatentable over Dan in view of Epsteine

Claim 1

The rejection of Independent Claim 1 is improper because (1) the cited references do not teach or suggest all of the claim elements and (2) there is no proper motivation to combine or modify the references to arrive at the claimed combination.

The references do not teach or suggest generating a plurality of virtual private proxies (VPPs). Claim 1 recites generating a plurality of VPPs based on an agreement between a first entity and a second entity. The Examiner asserts that this element is taught by Dan, specifically citing col. 5 lines 49-63 and col. 6 lines 11-25 of Dan. Appellant disagrees.

The VPP recited in the claim is not anticipated by elements of a system and network explicitly described as being public. Dan's disclosure of its enforcement code components does not teach or suggest generating a plurality of VPPs because Dan's enforcement code components are not VPPs. Whereas it is axiomatic that the claimed VPPs are private, Dan's enforcement code components are components of a business service application that Dan explicitly describes and praises as being public. Dan's enforcement code components 502, 504, and 506 are components of Dan's business service application 500. Business service application 500 corresponds to Dan's business service 400 as depicted in FIG 4. See Dan col. 5, lines 51-52.

Dan states unambiguously that the environment depicted in FIG 4, including business service 400, is a public environment. Moreover, Dan expressly declares the public nature of its environment to be an important aspect of Dan's application. See, e.g., Dan col. 5 lines 43-48. Appellant submits that a claim element reciting a VPP cannot be anticipated by the disclosure in a reference of enforcement code components expressly described as comprising a portion of a public application and environment.

The VPP recited in the claim is not anticipated by elements of a system and network explicitly that are clearly not proxies. In addition to not being private, the elements of Dan's system as depicted in FIG. 4 and FIG. 5 are not proxies. In the field of computer networks, a proxy machine or proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. See, e.g., the "proxy server" entry from Wikipedia. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache.

Neither the business service 400, the business service engine 402, the business service application 500, nor the enforcement code components 502, 504, and 506 of Dan qualify as proxies. Dan itself, for example, does not describe any of these components as proxies. Instead, Dan accurately describes the implementation of its business service (400) as a business service application (500). Dan's application 500 receives requests from a client engine 516 and enforces adherence to a service contract 514. One of ordinary skill would readily recognize a distinction between a software application such as Dan's business service application 500 and a proxy as claimed. Because Dan's enforcement code components are neither private nor proxies, Dan does not teach or suggest creating a plurality of VPPs. Accordingly, Appellant submits that the Section 103(a) rejection of Claim 1 is improper because the cited references do not teach or suggest all of the claim elements.

There is no motivation to modify Dan's public system using Epstein's firewall enhancement system. The rejection is further improper because there is no motivation to combine Dan and Epstein as the Examiner has done. Specifically, one of ordinary skill in the

field would not be motivated to modify Dan's publicly accessible business service application to implement Epstein's system for improving firewalls because doing so would undermine a basic operating principle of Dan, namely, that its business service application is designed and intended to be implemented across publicly available networks. Dan at col. 5, lines 43-48. Where a proposed modification to a reference would undermine a fundamental principle of operation of the reference, obviousness cannot be established under Section 103(a). See, e.g., MPEP 2143.01. Accordingly, Appellant respectfully submits that the Section 103(a) rejection of independent claim 1 is improper because there is no motivation to combine or modify Dan and Epstein as the Examiner suggests to arrive at the claimed combination. Appellant, therefore, respectfully requests the review panel to consider and reverse the Section 103(a) rejection.

In addition to the foregoing, Claim 1 is allowable over Dan and Epsteine because the references fail to disclose, expressly or inherently "determining whether the data violates the agreement." The Office Action points to Column 6, lines 25-47 of Dan as an alleged disclosure of this feature, but this is incorrect. This portion of Dan describes an automatic generation of code used to implement a service contract - not determining whether data violates the agreement. Other portions of Dan discuss enforcement code that:

> can log the request (noting time and content), number the request for correlation to an anticipated response, provide a signing function, include a timer function and notification in event of timeout and pass the request by a chosen protocol. When receiving a request or response from the service application 500, the enforcement code component can provide some of the functions listed hereinabove and also can determine whether the message is a response or a request, check validity of response and take appropriate action.(Dan, Column 6, lines 51-56).

This certainly is not determining whether the data violates the agreement. Furthermore, Appellant is unaware of a disclosure in Epsteine, which could reasonably be interpreted as a disclosure of determining whether the data violates the agreement. For at least this reason, Appellant submits that Independent Claim 1 and its dependents should be allowed.

In addition to the foregoing, Claim 1 is further allowable over Dan and Epsteine because the references fail to teach or suggest "disallowing communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement."

The Office Action acknowledged that Dan does not disclose this feature. Supporting the rejection, the Office Action relies on Epsteine, Column 8, Line 56 -Column 9, line 23, which reads:

> FIGS. 6A and 6B illustrate the sequences for a successful or unsuccessful protocol operation. Consider first the successful sequence of operations in FIG. 6A. The operation starts on the inside network 210, where a client application sends a request (Sl) to the inside listener/sender (proxy A) 512. Access controls may be performed at this step before the request is externalized into a file and transferred (S2) to content-based filter 516. Content-based filter 516 makes a decision based on the contents of the request, and forwards the file (S3) to the outside listener/sender (proxy B) 514. The file is then converted from the file format back into the original protocol format, and sent to the server on the outside network 220. When the server responds (S5), the outside listener/sender 514 may perform access controls, and then convert the response to a file. The file continues back through the content-based filter 5 16 (S6) to the inside listener/sender 5 12 (S7), where it is converted back into a protocol stream and sent to the originating client. (Epsteine, Column 8, Line 56 - Column 9, line 23).

The above passage provides no disclosure of disallowing communication of data from the first virtual private proxy to the second virtual private proxy when the data violates an agreement. Appellant submits that the Section 103(a) rejection is improper.

Claim 14

The rejection of Claim 14 is improper because the VPP recited in the claim is not anticipated by elements of a system and network explicitly described as being public. As argued above with respect to Claim 1, Dan's disclosure of its enforcement code components does not teach or suggest generating a plurality of VPPs because Dan's enforcement code components are not VPPs. Moreover, the VPP recited in the claim is not anticipated by elements of a system and network explicitly that are clearly not proxies. As argued above, neither the business service 400, the business service engine 402, the business service application 500, nor the enforcement

code components 502, 504, and 506 of Dan qualify as proxies. In addition, there is no motivation to modify Dan's public system using Epstein's firewall enhancement system. Again, one of ordinary skill in the field would not be motivated to modify Dan's publicly accessible business service application to implement Epstein's system for improving firewalls because doing so would undermine a basic operating principle of Dan. Accordingly, Appellant respectfully requests the review panel to consider and reverse the Section 103(a) rejection of Claim 14 and its dependent claims.

Claim 26

The rejection of Claim 26 is improper because the VPP recited in the claim is not anticipated by elements of a system and network explicitly described as being public. As argued above with respect to Claim 1, Dan's disclosure of its enforcement code components does not teach or suggest generating a plurality of VPPs because Dan's enforcement code components are not VPPs. Moreover, the VPP recited in the claim is not anticipated by elements of a system and network explicitly that are clearly not proxies. As argued above, neither the business service 400, the business service engine 402, the business service application 500, nor the enforcement code components 502, 504, and 506 of Dan qualify as proxies. In addition, there is no motivation to modify Dan's public system using Epstein's firewall enhancement system. Again, one of ordinary skill in the field would not be motivated to modify Dan's publicly accessible business service application to implement Epstein's system for improving firewalls because doing so would undermine a basic operating principle of Dan. Accordingly, Appellant respectfully requests the review panel to consider and reverse the Section 103(a) rejection of Claim 26 and its dependent claims.

Claim 41

The rejection of Claim 41 is improper because the VPP recited in the claim is not anticipated by elements of a system and network explicitly described as being public. As argued above with respect to Claim 1, Dan's disclosure of its enforcement code components does not

teach or suggest generating a plurality of VPPs because Dan's enforcement code components are not VPPs. Moreover, the VPP recited in the claim is not anticipated by elements of a system and network explicitly that are clearly not proxies. As argued above, neither the business service 400, the business service engine 402, the business service application 500, nor the enforcement code components 502, 504, and 506 of Dan qualify as proxies. In addition, there is no motivation to modify Dan's public system using Epstein's firewall enhancement system. Again, one of ordinary skill in the field would not be motivated to modify Dan's publicly accessible business service application to implement Epstein's system for improving firewalls because doing so would undermine a basic operating principle of Dan. Accordingly, Appellant respectfully requests the review panel to consider and reverse the Section 103(a) rejection of Claim 41 and its dependent claims.

The Section 103(a) rejection of Claims 8-10, 21-23, 27, 33-36, 42, and 55 as unpatentable over Dan in view of Epsteine, and further in view of Dan '103

Claim 8

The Section 103(a) rejection of Claim 8 is improper because the Examiner has failed to establish a prima facie case of obviousness. Claim 8 recites that the agreement includes the types of data allowed (to be exchanged between the entities via the VPPs). Appellant submits that this element is not taught or suggested by the cited references. The Office Action tacitly acknowledges the lack of teaching on this element because the Office Action does not even allege that the references teach or suggest this claim element. In numbered paragraph 28 of the Office Action, for example, the Office Action does not allege that Dan '103 teaches an agreement the includes the types of data allowed. Therefore, because the references do not teach or suggest all of the claim elements, the rejection is improper and should be reversed.

Claim 55

The rejection of Claim 55 is improper because the VPP recited in the claim is not anticipated by elements of a system and network explicitly described as being public. As argued above with respect to Claim 1, Dan's disclosure of its enforcement code components does not teach or suggest generating a plurality of VPPs because Dan's enforcement code components are not VPPs. Moreover, the VPP recited in the claim is not anticipated by elements of a system and network explicitly that are clearly not proxies. As argued above, neither the business service 400, the business service engine 402, the business service application 500, nor the enforcement code components 502, 504, and 506 of Dan qualify as proxies. In addition, there is no motivation to modify Dan's public system using Epstein's firewall enhancement system. Again, one of ordinary skill in the field would not be motivated to modify Dan's publicly accessible business service application to implement Epstein's system for improving firewalls because doing so would undermine a basic operating principle of Dan. Accordingly, Appellant respectfully requests the review panel to consider and reverse the Section 103(a) rejection of Claim 55 and its dependent claims.

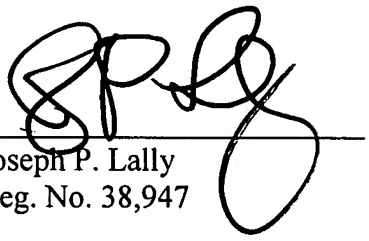
SUMMARY

Appellant requests the Board to review and reverse the rejections of the pending claims. Appellant authorizes the Commissioner to charge $500.00 for the Appeal Brief, a one-month

extension fee of $120.00, and any other fees necessary, or credit any overpayment to the Deposit Account of Jackson Walker L.L.P., No. 10-0096.

Respectfully submitted,

JACKSON WALKER L.L.P.
Attorneys for Appellant



Joseph P. Lally
Reg. No. 38,947

CORRESPONDENCE ADDRESS:
CUSTOMER NO. **67942**
JACKSON WALKER L.L.P.
512.236.2019
512.391.2111 (Fax)

VIII. CLAIMS APPENDIX

1. (Previously Presented) A method for secure communication comprising:

generating a plurality of virtual private proxies based on an agreement between a first entity and a second entity;

associating a first virtual private proxy of the plurality of virtual private proxies with the first entity and a second virtual private proxy of the plurality of virtual private proxies with the second entity;

monitoring data at the first virtual private proxy associated with the first entity;

determining whether the data violates the agreement; and

disallowing communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

2. (Previously Presented) The method for secure communication according to Claim 1, wherein determining whether the data violates the agreement comprises:

determining whether the data includes a security violation.

3. (Previously Presented) The method for secure communication according to Claim 2, wherein the security violation is a virus or malicious program.

4. (Previously Presented) The method for secure communication according to Claim 2, wherein the security violation is an intrusion attempt.

5. (Previously Presented) The method for secure communication according to Claim 1, further comprising:

hiding the existence of at least one of the first virtual private proxy or the second virtual private proxy to entities other than the first entity and the second entity of the agreement.

6-7. (Cancelled)

8. (Original) The method for secure communication according to Claim 1, wherein the agreement comprises types of data allowed.

9. (Original) The method for secure communication according to Claim 8, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication and wherein the type of data allowed comprises XML data.

10. (Original) The method for secure communication according to Claim 9, wherein the agreement further comprises a document exchange protocol indication and a process specification document indication.

11-13. (Cancelled)

14. (Previously Presented) A system for secure communication comprising:

logic stored on a medium and configured to:

generate a plurality of virtual private proxies based on an agreement between a first entity and a second entity;

associate a first virtual private proxy of the plurality of virtual private proxies with the first entity and a second virtual private proxy of the plurality of virtual private proxies with the second entity;

monitor data at the first virtual private proxy associated with the first entity;

determine whether the data violates the agreement; and

disallow communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

15-20. (Cancelled)

21. (Previously Presented) The system for secure communication according to Claim 14, wherein the logic is further configured to:

receive a first profile from the first entity;

receive a second profile from the second entity; and

automatically generate the agreement based on the first profile and the second profile.

22. (Original) The system for secure communication according to Claim 21, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication and wherein the type of data allowed comprises XML data.

23. (Original) The system for secure communication according to Claim 22, wherein the agreement further comprises a document exchange protocol indication and a process specification document indication.

24. (Previously Presented) The system for secure communication according to Claim 14, wherein the logic in determining whether the data violates the agreement determines whether the data includes an intrusion attempt.

25. (Previously Presented) The system for secure communication according to Claim 14, wherein the logic in determining whether the data violates the agreement determines whether the data includes a virus or malicious program.

26. (Original) A method for secure communication comprising:

generating a first virtual private proxy associated with a first entity;

generating a second virtual private proxy associated with a second entity;

monitoring communications between the first virtual private proxy and the second virtual private proxy based on an agreement for electronic data exchange between the first and second entities; and

responding to violations of the agreement based on the agreement.

27. (Original) The method according to Claim 26 and further comprising:

determining a first profile associated with the first entity;

determining a second profile associated with the second entity; and

automatically generating the agreement based on the first and second profiles.

28. (Original) The method according to Claim 26 and further comprising:

linking the first virtual private proxy to the second virtual private proxy over a link; and

communicating data between the first virtual private proxy and the second virtual private proxy over the link.

29. (Original) The method according to Claim 28, wherein the link comprises a logical data link at a secure switch.

30-32. (Cancelled)

33. (Previously Presented) The method according to Claim 27, wherein the first profile comprises at least one indication of business information associated with the first entity.

34. (Previously Presented) The method according to Claim 27, wherein the first profile comprises a transport protocol and a messaging protocol.

35. (Original) The method according to Claim 34, wherein the first profile further comprises a transport security protocol and a specification document.

36. (Original) The method according to Claim 35, wherein the first profile further comprises a name and contact information associated with the first entity.

37. (Original) The method according to Claim 26, wherein determining the violation comprises:

examining the data with respect to the agreement at the first virtual private proxy;

determining whether the data is allowed by the agreement;

determining the violation when the data is not allowed by the agreement; and

communicating the data to the second virtual private proxy when the data is allowed by the agreement.

38. (Original) The method according to Claim 26, wherein responding to the violation comprises:

generating an alarm based on the violation;

logging the violation; and

discarding the data associated with the violation.

39. (Original) The method according to Claim 38, wherein responding to the violation further comprises forbidding communication between the first virtual private proxy and the second virtual private proxy.

40. (Cancelled)

41. (Previously Presented) A system for secure communication comprising:

logic stored on storage and configured to:

generate a first virtual private proxy associated with a first entity;

generate a second virtual private proxy associated with a second entity;

monitor communications between the first virtual private proxy and the second virtual private proxy based on an agreement for electronic data exchange between the first and second entities; and

respond to violations of the agreement based on the agreement.

42. (Previously Presented) The system according to Claim 41, wherein the logic is further configured to:

determine a first profile associated with the first entity;

determine a second profile associated with the second entity; and

automatically generate the agreement based on the first and second profiles.

43. (Previously Presented) The system according to Claim 41, wherein the logic is further configured to:

link the first virtual private proxy to the second virtual private proxy over a link; and

communicate data between the first virtual private proxy and the second virtual private proxy over the link.

44-46. (Cancelled)

47. (Previously Presented) The system according to Claim 41, wherein the logic is further configured to:

hide the existence of at least one of the first virtual private proxy or the second virtual private proxy to entities other than the first entity and the second entity of the agreement.

48. (Previously Presented) The system according to Claim 42, wherein the first profile comprises at least one indication of business information associated with the first entity.

49. (Previously Presented) The system according to Claim 42, wherein the first profile comprises a transport protocol and a messaging protocol.

50. (Original) The system according to Claim 49, wherein the first profile further comprises a transport security protocol and a specification document.

51. (Original) The system according to Claim 50, wherein the first profile further

comprises a name and contact information associated with the first entity.

52. (Previously Presented) The system according to Claim 41, wherein the agreement prohibits viruses or malicious programs.

53. (Previously Presented) The system according to Claim 41, wherein the agreement prohibits intrusion attempts.

54. (Previously Presented) The system according to Claim 53, wherein the logic is further configured to forbid communication between the first virtual private proxy and the second virtual private proxy.

55. (Previously Presented) A method for secure communication comprising:

generating a plurality of virtual private proxies based on an agreement between a first entity and a second entity;

wherein the agreement further comprises a document exchange protocol indication and a process specification document indication;

associating a first virtual private proxy of the plurality of virtual private proxies with the first entity and a second virtual private proxy of the plurality of virtual private proxies with the second entity;

wherein the first virtual private proxy comprises a logical representation of a logical access point between the first entity and a secure switch;

monitoring data at the first virtual private proxy associated with the first entity;

examining the data with respect to the agreement at the first virtual private proxy;

determining whether the data is allowed by the agreement;

indicating a violation when the data does not conform to the agreement;

and disallowing communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

56. (Withdrawn) A method for secure communication, the method comprising:

communicating a profile to a secure switch, the profile specifying parameters of communication;

initiating a connection with a secure switch; and

receiving data through a first virtual private proxy of the secure switch that complies with the parameters specified by the profile.

57. (Withdrawn) The method of Claim 56, wherein the communicating, initiating, and receiving are carried out on a first entity and the profile is associated with the first entity.

58. (Withdrawn) The method of Claim 57, further comprising:

receiving, at the first entity, a communication initiation request from a remote computer; and

facilitating communication between the remote computer and a second entity.

59. (Withdrawn) The method of Claim 57, further comprising: communicating data, from the first entity, to a second entity through the secure switch.

60. (Withdrawn) The method of Claim 59, further comprising:

receiving an indication from the secure switch that the communicated data does not comply with parameters specified by a profile of the second entity.

61. (Withdrawn) The method of Claim 57, wherein the received data is communicated from a second entity through the secure switch.

62. (Withdrawn) The method of Claim 56, wherein the profile is used in a Collaboration Profile Agreement.

63. (Withdrawn) The method of Claim 56, wherein the profiles specifies a type of

data.

64. (Withdrawn) The method of Claim 56, wherein the profiles prohibits viruses or malicious programs.

65. (Withdrawn) The method of Claim 56, wherein the profiles prohibits intrusion attempts.

66. (Withdrawn) The method of Claim 56, wherein the connection is a secure connection.

67. (Withdrawn) A system for secure communication comprising:

logic stored on computer readable media and configured to:

communicate a profile to a secure switch, the profile specifying parameters of communication;

initiate a connection with a secure switch; and

receive data through a first virtual private proxy of the secure switch that complies with the parameters specified by the profile.

68. (Withdrawn) The system of Claim 67, wherein the logic is associated with a first entity.

69. (Withdrawn) The system of Claim 68, wherein the logic is further configured to:

receive a communication initiation request from a remote computer; and

facilitate communication between the remote computer and a second entity.

70. (Withdrawn) The system of Claim 68, wherein the logic is further configured to:

receive an indication from the secure switch that the communicated data does not comply with parameters specified by a profile of the second entity.

71. (Withdrawn) The system of Claim 67, wherein the profiles specifies a type of data.

72. (Withdrawn) The system of Claim 67, wherein the profiles prohibits viruses or malicious programs.

73. (Withdrawn) The system of Claim 67, wherein the profiles prohibits intrusion attempts.

IX. EVIDENCE APPENDIX

NONE

X. RELATED PROCEEDINGS APPENDIX

NONE